AMENDMENT

Please replace all prior versions and listings of claims with the following listing of claims.

LISTING OF CLAIMS:

1. (**Currently Amended**) A method ~~of monitoring~~ for detecting and preventing attacks directed at a target system ~~network communications for an indication of an attack and disabling the network communications upon an existence of a predetermined condition~~, comprising:

receiving one or more packets originating from a source system, the received packets directed to the target system;

~~monitoring data packets received at a target system in real time;~~

monitoring ~~identifying~~ the received ~~data~~ packets ~~that are~~ to identify one or more of the packets that include information associated with ~~signatures of the~~ a signature of an attack directed at the target system;

~~determining a severity of the attack; and~~

blocking the identified packets from being transmitted to the target system; and

blocking one or more subsequently received ~~the data~~ packets from ~~entering~~ being transmitted to the target system when ~~the~~ a severity of the attack exceeds a predetermined threshold, the subsequently blocked packets including one or more of packets originating from the source system or directed to the target system.

2. (**Currently Amended**) The method according to claim 1, wherein monitoring the ~~data~~ packets includes determining ~~received at the target system are monitored based on~~ at least one of identifying information ~~and~~ or a type of communication associated with the monitored packets.

3. (**Currently Amended**) The method according to claim 2, wherein the identifying information includes at least one of a source ~~an~~ Internet Protocol address, a source port number, a destination Internet Protocol address, or a destination ~~and~~ a port number.

4. (**Currently Amended**) The method according to claim 2, wherein the type of communication includes at least one of [[a]] File Transfer Protocol, [[a]] Simple Mail Transfer Protocol, Telnet, Domain Name System, Windows Internet Name System, HyperText Transfer Protocol, Traceroute, instant messaging, ~~and~~ or chat.

5. (**Currently Amended**) The method according to claim 1, wherein monitoring the ~~data~~ packets includes ~~received at the target system are monitored~~ using Transmission Control Protocol/Internet Protocol at an application layer.

6. (**Currently Amended**) The method according to claim 1, further comprising determining ~~wherein~~ the severity of the attack ~~is determined~~ based on at least one of a frequency of the attack, a type of communication, a change in an amount of bandwidth, ~~and~~ or a volume of the received ~~data~~ packets.

7. (**Currently Amended**) The method according to claim 1, wherein blocking the ~~data~~ packets from being transmitted to ~~are blocked from entering~~ the target system ~~by~~ includes instructing at least one of a router, a hub, a server, ~~and~~ or a firewall to disable a communication channel.

8. (**Currently Amended**) The method according to claim 1, further comprising ~~the step of~~ notifying ~~an attacking~~ the source system ~~of a detection of~~ that the attack has been detected and that ~~of blocking the data~~ packets subsequently sent from the ~~attacking~~ source system will be blocked.

9. (**Currently Amended**) The method according to claim 1, wherein the subsequently received ~~data~~ packets are blocked from ~~entering~~ being transmitted to the target system for a predetermined amount of time.

10. (**Currently Amended**) A system for protecting a computer network, comprising at least one computer readable medium associated with a device coupled to the network, the computer readable medium including:

a detection module that receives attack signatures associated with attacks directed at a target device ~~data packets~~ and monitors received ~~data~~ packets to identify one or more of the packets that include information associated with ~~for~~ the attack signatures;

a scanning module that evaluates the ~~received data~~ identified packets ~~having the attack signatures and determines~~ to determine a severity of an attack on the ~~computer network~~ target device; and

a blocking module that identifies a source of the ~~attack~~ identified packets, ~~and~~ instructs at least one ~~switching~~ device to block the ~~data~~ identified packets from being transmitted to the target device, and instructs the at least one device to block one or more subsequently received packets from being transmitted to the target device when ~~associated with the attack signatures~~ ~~if~~ the severity of the attack exceeds a predetermined threshold, the subsequently blocked packets including one or more of packets originating from the source or directed to the target device.

11. (**Currently Amended**) The system according to claim 10, wherein the computer readable medium further includes ~~comprising~~ a log module that ~~is adapted to create~~ creates a log of the ~~received data~~ packets identified as including the information associated with ~~having~~ the attack signatures.

12. (**Currently Amended**) The system according to claim 10, wherein the detection module ~~is adapted to monitor~~ monitors the received ~~data~~ packets ~~based on~~ by determining at least one

of identifying information ~~and~~ or a type of communication associated with the monitored packets.

13. (**Currently Amended**) The system according to claim 10, wherein the scanning module ~~is adapted to determine~~ determines the severity of the attack based on at least one of a frequency of the attack, a type of communication, a change in an amount of bandwidth, ~~and~~ or a volume of the received ~~data~~ packets.

14. (**Currently Amended**) The system according to claim 10, wherein the blocking module blocks ~~data~~ the packets from being transmitted to the target device ~~entering the computer network~~ by instructing at least one of a router, a hub, a server, ~~and~~ or a firewall to disable a communication channel.

15. (**Currently Amended**) The system according to claim 14, wherein the blocking module blocks the ~~data~~ packets from being transmitted to the target device ~~entering the computer network~~ for a predetermined amount of time.

16. (**Currently Amended**) A computer readable medium containing computer executable instructions ~~program product~~ for detecting and preventing attacks directed at a target system ~~enabling a computer to monitor received data packets and to disable a transmission medium between a source computer and a destination network upon an existence of a predetermined condition~~, the computer executable ~~program product having~~ instructions ~~for enabling the computer to perform operations comprising~~ operable to:

receive one or more packets originating from a source system, the received packets directed to the target system;

~~monitoring data packets received at a destination network;~~

monitor ~~identifying~~ the received ~~data~~ packets ~~that are~~ to identify one or more of the packets that include information associated with ~~signatures~~ a signature of an attack directed at the target system;

~~determining a severity of the attack; and~~

block the identified packets from being transmitted to the target system; and

block one or more subsequently received ~~blocking the data~~ packets from ~~entering~~ being transmitted to the target system ~~destination network~~ when ~~the~~ a severity of the attack exceeds a predetermined threshold, the subsequently blocked packets including one or more of packets originating from the source system or directed to the target system.

17. (**Currently Amended**) The computer readable medium ~~program product~~ according to claim 16, wherein the received ~~data~~ packets are monitored transparently in real time.

18. (**Currently Amended**) The computer readable medium ~~program product~~ according to claim 16, wherein the received ~~data~~ packets are monitored after being stored in a storage buffer.

19. (**Currently Amended**) The computer readable medium ~~program product~~ according to claim 16, the instructions further operable to determine ~~wherein~~ the severity of the attack ~~is determined~~ based on at least one of a frequency of the attack, a type of communication, a change in an amount of bandwidth, ~~and~~ or a volume of the received ~~data~~ packets.

20. (**Currently Amended**) The computer readable medium ~~program product~~ according to claim 16, the instructions operable to block ~~wherein~~ the ~~data~~ packets ~~are blocked~~ from being transmitted to ~~entering~~ the target system by instructing at least one of a router, a hub, a server, ~~and~~ or a firewall to disable a communication channel.

21. (**Currently Amended**) The computer readable medium ~~program product~~ according to claim 16, the instructions further operable to notify the ~~comprising the step of notifying an attacking~~ source system ~~of a detection of~~ that the attack has been detected and that ~~of blocking the data~~ packets subsequently sent from the ~~attacking~~ source system will be blocked.

22. (**Currently Amended**) The computer readable medium ~~program product~~ according to claim 16, ~~wherein~~ the instructions operable to block the ~~data~~ packets ~~are blocked~~ from being transmitted to ~~entering~~ the target system for a predetermined amount of time.

23. (**Currently Amended**) A computer system configured for detecting and preventing attacks directed at target devices ~~to monitor data packets received on a transmission medium for an indication of an attack and to block receipt of the data packets upon an existence of a predetermined condition~~, comprising:

at least one terminal device;

~~an application server that is coupled to the at least one terminal device for processing requests sent by the at least one terminal device;~~

at least one ~~a monitoring~~ server ~~that is~~ coupled to a computer network and to the ~~application server for~~ terminal device, the server operable to ~~monitoring data~~ monitor packets directed to the terminal device, the ~~monitoring~~ server having one or more modules ~~comprising,~~ including:

a ~~first~~ detection module that receives attack signatures associated with attacks directed at the terminal device ~~data~~ packets and monitors received ~~data~~ packets to identify one or more of the packets that include information associated with ~~for~~ the attack signatures;

a ~~second~~ scanning module that evaluates the ~~received data~~ packets ~~having the attack signatures and determines~~ to determine a severity of an attack on the ~~computer system~~ terminal device; and

a ~~third~~ blocking module that identifies a source of the ~~attack~~ identified packets, ~~and~~ instructs at least one switching device to block the ~~data~~ identified packets from being transmitted to the terminal device, and instructs the at least one switching device to block one or more subsequently received packets from being transmitted to the terminal device when ~~associated with the attack signatures if~~ the severity of the attack exceeds a predetermined threshold, the subsequently blocked packets including one or more of packets originating from the source or directed to the terminal device.

24. (**Currently Amended**) The computer system according to claim 23, wherein the ~~monitoring~~ server further ~~comprises~~ includes a ~~fourth~~ log module that creates a log of the ~~received data~~ packets identified as including the information associated with ~~having~~ the attack signatures.

25. (**Currently Amended**) The computer system according to claim 23, further comprising a database coupled to the ~~monitoring~~ server.

26. (**Currently Amended**) The computer system according to claim 23, wherein the ~~first~~ detection module ~~is adapted to monitor~~ monitors the received ~~data~~ packets ~~based on~~ by determining at least one of identifying information ~~and~~ or a type of communication associated with the monitored packets.

27. (**Currently Amended**) The computer system according to claim 23, wherein the ~~third~~ scanning module ~~is adapted to determine~~ determines the severity of the attack based on at least one of a frequency of the attack, a type of communication, a change in an amount of bandwidth, ~~and~~ or a volume of the received ~~data~~ packets.

28. (**Currently Amended**) The computer system according to claim 23, wherein the ~~fourth~~ blocking module blocks data packets from being transmitted to the terminal device ~~entering the computer network~~ by instructing at least one of a router, a hub, a server, ~~and~~ or a firewall to disable a communication channel.

29. (**Currently Amended**) The computer system according to claim 23, wherein the ~~fourth~~ blocking module blocks the ~~data~~ packets from being transmitted to the terminal device ~~entering the network computer~~ for a predetermined amount of time.

30. (**Currently Amended**) The computer system according to claim 23, ~~wherein~~ the ~~monitoring~~ server further operable to issue ~~issues~~ an alert to inform an administrator of the network of the attack on the ~~computer system~~ terminal device.

31. (**New**) The method according to claim 3, the subsequently blocked packets including packets associated with one or more of the source Internet Protocol address, the source port number, the destination Internet Protocol address, or the destination a port number.